Tomasz HYLA, Włodzimierz BIELECKI, Jerzy PEJAŚ
WEST POMERANIAN UNIVERSITY OF TECHNOLOGY, FACULTY OF COMPUTER SCIENCE,
ul. Żołnierska 49, 71-200 Szczecin

Non-repudiation of Electronic Health Records in distributed healthcare systems

M.Sc. Tomasz HYLA

Ph.D. student of the Software Technology Department of the West Pomeranian University of Technology, Szczecin. He received M.Sc. degree in Computer Science and Engineering from the Szczecin University of Technology in 2007. His research interest includes: IT security applied to electronic health records (EHRs), security of long-term electronic archives and confidentiality in distributed systems.

e-mail: thyla@wi.zut.edu.pl

Prof. Włodzimierz BIELECKI

He is a head of the Software Technology Department of the West Pomeranian University of Technology, Szczecin. His research interest includes parallel and distributed computing, optimizing compilers, extracting both fine- and coarse grained parallelism available in program loops.

e-mail: wbielecki@wi.zut.edu.pl

Ph.D. eng. Jerzy PEJAŚ

He received M.Sc. degree in Computer Science and Engineering from the Wrocław University of Technology and Ph.D. degree in Control Systems from Gdansk University of Technology. Main subjects of interest: information and computer network security, methods of secure electronic signatures as well as new trends in applied cryptography. Employed as Associate Professor at the Faculty of Computer Science and Information Technology, West Pomeranian University of Technology, Szczecin.

e-mail: jpejas@wi.zut.edu.pl

Abstract

Healthcare systems managing Electronic Health Records (EHR) are being implemented around the world to facilitate access to patients' health data. The primary idea of the EHR is to gather all health information about a subject of care in one place. When a countrywide EHR system is fully implemented, it is assumed that all newly created documentation is stored in the system. Distributed healthcare systems, which connect national or regional healthcare system, are necessary to allow access to patient' health data in any of connected nationwide healthcare systems. In such complex systems, due to high commercial value and sensitiveness of medical data, security is a very important issue. The paper presents a solution for maintaining evidence records, which can ensure a non-repudiation of EHR content, stored in many nationwide systems. In other words, the verifier using the registry evidence records can proof the non-repudiation of EHR content, which is stored outside a patient home healthcare system.

Keywords: EHR, long-term storage, non-repudiation, healthcare.

Niezaprzeczalność elektronicznych dokumentów zdrowotnych w rozproszonych systemach ochrony zdrowia

Streszczenie

Systemy ochrony zdrowia zarządzające elektronicznymi dokumentami zdrowotnymi (EHR) są wdrażane na całym świecie w celu ułatwienia dostępu do danych o zdrowiu pacjentów. Podstawową ideą EHR jest zebranie wszystkich informacji medycznych dotyczących jednego pacjenta w jednym miejscu. Gdy ogólnokrajowy system EHR jest w pełni wdrożony, zakłada się, że wszystkie nowo utworzone dokumenty są przechowywane w systemie. Rozproszone systemy ochrony zdrowia łączące narodowe lub regionalne systemy ochrony zdrowia są konieczne aby umożliwić specjalistom ds. ochrony zdrowia dostęp do wszystkich danych dotyczących jednego pacjenta. W tak skomplikowanych systemach, z uwagi na dużą wrażliwość danych medycznych i ich dużą wartość komercyjną np. na rynku ubezpieczeń, bezpieczeństwo jest jednym z głównych priorytetów. W artykule przedstawiono rozwiązanie pozwalające na zarządzanie rekordami poświadczeń rejestrów, za pomocą których można wykazać niezaprzeczalność zawartości EHR, przechowywanego w wielu ogólnokrajowych systemach EHR. Zewnętrzny weryfikator używając rekordów poświadczeń rejestrów może wykazać, że zawartość EHR jest oryginalna i niezmodyfikowana.

Słowa kluczowe: EHR, długoterminowe przechowywanie, niezaprzeczalność, ochrona zdrowia.

1. Introduction

The EHR (Electronic Health Record) is a virtual container for healthcare documents related to one subject of care. Health information has a high commercial value to some parts of the industry, e.g. insurance companies. Disclosure of private health information, like some psychologies episodes, to an employer might have a negative influence for an employee. The availability of all health information related to one patient in a single point of access requires proper security measures. From the other side, the idea of an EHR is to provide to an authorized physician a patient medical history from a cradle to a grave. The transition from a paper based documentation and from an electronic documentation stored in separate systems to the EHRs can reduce many medical errors and improve a healthcare quality [1, 2].

The primary idea of the EHR is to gather all health information about a subject of care in one place. When the countrywide EHR system is fully implemented, it is assumed that all newly created documentation is stored in the EHR system. In practice, EHR content is made of many documents, which usually are stored in many registries and repositories, which might belong to different healthcare organizations. The EHR system must have a service for querying and retrieving documents from patients' EHRs.

Nowadays, the development of nationwide healthcare systems is a priority of many countries around the world. In the European Union, due to the European Commission directives and plans for development of an information society, a pan-European EHR system is a long-term goal. An EHR system manages and allows access to the EHR. The security of such complex system, which must process data from hundreds of millions people, is a major concern. Also, international systems must have built in solutions for solving security problems related to different national legislations.

A solution responsible for transfer, creation and verification of Registry Evidence Records (RERs) and messages necessary to maintain RERs within all associated EHR system is proposed in this paper. The proposed solution enables external verification of EHR content. The second section of this paper contains introduction to EHRs, EHR systems and security issues with emphasis on a non-repudiation property. The third section introduces proposed algorithms while the 4th section contains summary and discussion.

2. Background

2.1. EHR systems

A few logical models of EHR system architectures are available, e.g. openEHR [3], CEN/ISO 13606-1 [4]. In the

CEN/ISO 13606-1 logical information model on a higher level in a component hierarchy is an EHR_Extract component. The EHR_Extract contains optional folders used to logically group compositions. One folder can contain zero or more compositions. A composition is an equivalent of a clinical document (e.g. blood test results, a prescription) and it is a smallest unit of information that can be added or exchanged. If it is necessary to correct data in one of compositions, a new composition must be added and marked as the latest version. The EHR_Extract is created upon request and might contain few chosen compositions or all of them. If contains all composition, then includes a complete patient's EHR.

In the world an adoption rate and functionality of national (regional) EHR systems varies. Different local conditions, policies and requirements result in different approaches to the design of EHR systems. An international (inter-regional) EHR system can span many national (regional) systems to provide better access to patient medical data. The main question in a design of such system is where to store the EHR's. There are three basic possibilities to store data [5]:

- locally – clinical documents are stored in many different local systems (hospital, laboratory, GP systems) and are only registered in a central EHR systems' registry, only metadata is stored in the EHR system;
- centrally – clinical documents are stored inside EHR system repositories;
- hybrid – locally plus centrally.

EHR systems can be built based on the IHE Cross-Enterprise Document Sharing (XDS) [6]. IHE XDS is a specification created for sharing documents between healthcare enterprises based on established standards, including repositories and registries standards.

2.2. EHR security

The EHR system implementation must fulfil many security requirements. Generic requirements for EHR systems are stated in the ISO TS 18308 [7]. H. Linden et al. in [8] listed the most relevant security requirements. Clinical documents stored in patients' EHRs should be digitally signed to meet security requirements such as integrity, authenticity and non-repudiation.

EHR must be stored for an entire life of a patient, which can be even 100 years. Document cannot be deleted from the EHR, because the ISO 18308 requires the existence of a possibility to restore the view of an EHR in any previous point of time. The EHR storage period is much longer then validity period of a digital signature, which is usually two years. During that period a method preserving the validity of digital signatures is required, because the digital signatures are valid as long as are valid evidences related to them.

The method for preserving the validity of a single signature is described in a XML Advanced Electronic Signatures specification (XAdES) [9]. An EHR system can store billions of documents. Extension of validity period using XAdES for such a number of signed documents requires a lot of processing power, because each signature is processed separately. Due to that fact, a few solutions which resign or timestamp a group of signed documents, were presented by Pharow and Blobel [10] and by Blazic et al. [11]. The timestamps and digital signatures used in the resigning process are used to confirm the technical validity of a document and previous signatures.

One of the most complex solutions of extending the signature validity is provided in RFC 4998 "Evidence Record Syntax (ERS)" [12] and in its XML version [13]. ERS describes the evidence records structure and processing methods. Evidence records are a set of data needed to prove the data existence. Document is time stamped before expiration of a digital signature. Archive timestamps might cover a single document or group of documents, which are concatenated using Merkle Hash Tree [14]. Timestamp is required only for a root hash when using such a hash tree.

2.3. Non-repudiation of the EHR

One of the most important security requirements is non-repudiation – a property *"allowing any actor to obtain proof, which cannot be forged, that confirms the integrity and origin of a data item"* [8]. In this paper is assumed a data item as the EHR. Non-reputation of the EHR guarantees that the EHR is coherent, its content is original and was not modified.

The EHR is virtual one in this sense that it is crated upon request from user based on query details. The content of the EHR is usually stored using registry/repository model with one central, logical registry that contains information about localization of all documents. Based on that information central registry can retrieve all documents which are related to requested patient, recreate and send the EHR to query originator. When metadata stored in some of registries is modified or deleted, then query result might not return some of documents. False query result means that important clinical documents might be unavailable and as a result a physician can misdiagnose a patient.

The non-repudiation property of clinical documents stored in repositories can be achieved using methods described in Section 2.2. However, these methods cannot be directly applied to registries. In [15] is described the algorithm for maintaining non-repudiation of registries entries related to one patient. The algorithm use Merkle hash tree, ERS and mechanisms of linear evidence linking. New entries in the registry are grouped into rounds specified by time period or maximum number of new entries. Firstly, combined hash H^i_n is calculated for each new *n-th* entry in the registry linked with *i-th* patient. Next, a value $L^i_n = H(n \,||\, H^i_n \,||\, L^i_{n-1} \,||\, T^i_{n-1})$ is calculated, where T^i_{n-1} is a timestamp linked with *i*-th patient' last entry or last group of entries. Then, using L^i_n from all patient which took part in the round, the Merkle hash tree is calculated using ERS. The root is relayed to the Time Stamp Authority, which creates linked time stamp token TS_n. These tokens are relayed to the registry and stored together with a reduced hash tree in the entry linked with L^i_n value.

3. Non-repudiation in a distributed environment

EHR systems are usually built using modular design. The EHR system can cover one country or region, depending on local conditions. Due to the fact that people travel to different countries/regions and use medical assistance outside their home EHR system, it is necessary to connect all the systems. It is a long-term goal of EU that all existing and future EHR systems of member countries should be connected.

The general architecture of the EHR system with necessary security "building blocks" is presented in [5]. The system connect with outside environment using four buses (see also Fig. 1):

1. auxiliary system bus – the bus uses to connect to other system, e.g. PKI services, national health organization;
2. external data bus – the bus used to connect to external repositories (when in the EHR system are only stored metadata in the registries and documents are stored in the local systems e.g. hospitals);
3. inter-jurisdiction bus – the bused for communication with other EHR systems in the same or different jurisdiction;
4. user access bus – single point of access for users i.e. healthcare professionals and patients.

The Integrated Care EHR service manages EHRs in a long time period. EHR index registry is a central registry, which contains references to all registries in the system. Query to that registry enables to retrieve all documents related to one patient. If a patient has documents in external systems (all systems outside patient home EHR system), then the Location Registry stores that information.

3.1. Registry Evidence Records

The Integrated Care EHR service contains Registry Security System (see Fig. 1) responsible for managing the Registry Evidence Records (RERs). RERs are used to proof the non-repudiation of EHRs and for prolonging the validity of digital signatures of clinical documents stored in repositories. The Registry Evidence Records update is performed using two algorithms:

1. The addition algorithm, which operate in a registry logical level, (e.g. algorithm from [15]) responsible for direct modification of RER;
2. The algorithm for clinical document addition, which operate in a EHR systems' logical level in a distributed environment; responsible for transfer, within all associated EHR system, of messages necessary to maintain RERs. This algorithm is presented further in Section 3.2.

The RERs are stored in Long-term Security Database. A single RER is a XML document, which stores hashes calculated from metadata sets and timestamps. It is possible to verify the non-repudiation of each EHR, using the RER and metadata from the EHR Central registry. Every patient has in his home system a RER calculated for all his clinical documents stored inside the system (see Fig. 1: *Home RER)* and abstracts from RERs stored in external systems (*External RER*). Also, in the database are stored *Guest RERs* – the RERs of patients from other EHR systems, which are temporarily using healthcare services (e.g. during vacation trip).

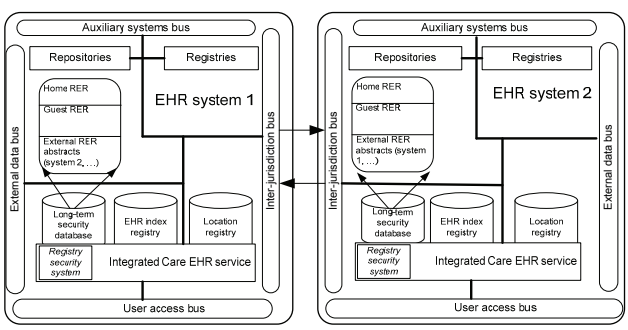

Fig. 1. Registry Evidence Records in the EHR system architecture
Rys. 1. Rekordy poświadczeń rejestrów w architekturze systemu EHR

The following abbreviations are used in next sections:

- D_i - clinical document number i – a clinical document which is send by a physician to the EHR system;
- $EHRS_h$ – home EHR system – the EHR system in which a patient is registered, i.e. system which operate in the patient' region of residence;
- $EHRS_k$ – external EHR system k – the EHR system which is connected to patient' home EHR system, i.e. system in another country/region;
- $ICEHR_h$ - Integrated Care EHR service in $EHRS_h$;
- $ICEHR_k$ - Integrated Care EHR service in $EHRS_k$;
- $LTSDB_h$ – Long-Term Security Database in $EHRS_h$;
- $LTSDB_k$ – Long-Term Security Database in $EHRS_k$;
- M_j^k – a message from EHR_k *to* EHR_h that P_j has clinical documents in $EHRS_k$;
- MS_i – Metadata Set which describe D_i;
- MS_i^k – MS_i after modification and stored in $EHRS_k$, the modification includes URI_i;
- MS_j^k – the collection of all MS_i^k stored in $EHRS_k$ which belong to P_j;
- MS_j – the collection of all MS_j^k from all $EHRS_k$ and from $EHRS_h$;
- P_j – Patient with id j;
- R_n – Registry with number n;
- RER_j – Registry Evidence Records of P_j;
- $RERj'$ – RER_j after update;
- RER_j^k - RER_j of P_j in $EHRS_k$;
- $aRER_j^k$ – abstract of $RERj'$ from $EHRS_k$;
- RSS_k – Registry Security Subsystem in $EHRS_k$;
- RSS_h – Registry Security Subsystem in $EHRS_h$;
- URI_i – Unified Resource Identifier to D_i in a repository.

3.2. RER update in external systems

When a clinical document is added to the patient' external EHR system, the RERs are updated inside the originating system and information is sent to the patient home system. The detailed algorithm is as follows (compare Fig. 2):

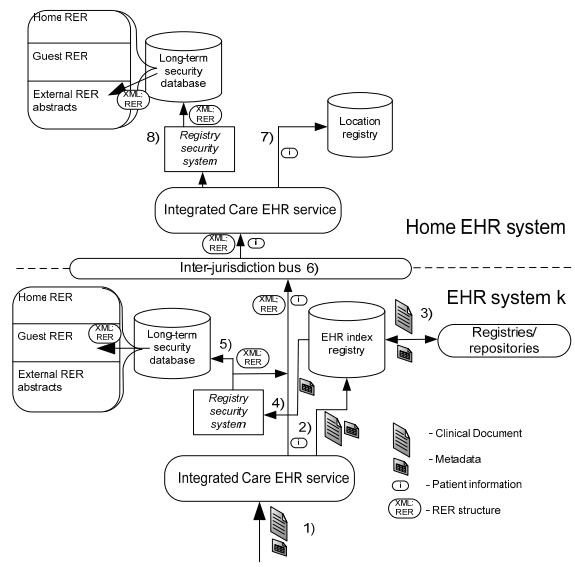

Fig. 2. Addition of a new document and RER update
Rys. 2. Dodanie nowego dokumentu i aktualizacja RER

Step 1. Healthcare professional sends a new document D_i and a MS_i related to patient P_j to $ICEHR_k$ in $EHRS_k$;

Step 2. $ICEHR_k$ sends D_i and M_i to EHR index registry and message M_j^k to inter-jurisdiction bus;

Step 3. EHR index registry adds an information about destination registry R_n to the records of P_j and sends further D_i and MS_i to R_n;

Step 4. EHR index registry modifies MS_i (by extracting additional metadata and inserting URI_i) and by that creates MS_i^k which sends to RSS_k;

Step 5. RSS_k retrieves a RER_j form $LTSDB_k$ from *Guest EHR* table or if not exists - creates new empty one; RSS_k run entry addition algorithm, which updates RER_j structure using incoming MS_i^k; RSS_k sends modified $RERj'$ to $LTSDB_k$ and creates $aRER_j^k$ which is send to the inter-jurisdiction bus;

Step 6. Using inter-jurisdiction bus, which mediate through EHR systems, M_j^k and $aRER_j^k$ are send to $ICEHR_h$ in $EHRS_h$;

Step 7. M_j^k is send to and registered in Location Registry in $EHRS_h$;

Step 8. $ICEHR_h$ sends $aRER_j^k$ to RSS_h, which run the entry addition algorithm and stores it inside *External RER abstract* table.

When a clinical document is added in a home system, the above algorithm is run without the steps 6-8 and in steps 2, 5 without sending data to inter-jurisdiction bus. Also in step 5 the *Home RER* table is used instead of the *Guest RER* table.

3.3. RER verification

The Registry Evidence Record verification is performed using two algorithms. First algorithm is responsible for verification of

RER XML file and second one is responsible for generating the RER XML file. This paper presents the second one – algorithm for generation of a RER xml file (see Fig. 3). When a user requests the RER XML file to verify EHR non-repudiation the home system gathers proofs from its system and from all external system in which patient has stored documents. The detailed algorithm is as follows (for abbreviations see Section 3.1):

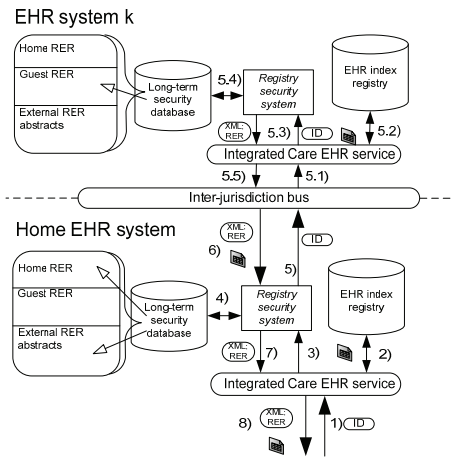

Fig. 3. Verification of Registry Evidence Records
Rys. 3. Weryfikacja Rekordów Poświadczeń Rejestrów

Step 1. The user sends request to $ICEHR_h$ for the RER_j;
Step 2. $ICEHR_h$ sends request to EHR index service for all metadata related to P_j;
Step 3. $ICEHR_h$ sends request to RSS_h for the RER_j;
Step 4. RSS_h retrieves from $LTSDB_h$ RER_j (from *Home RER* table);
Step 5. RSS_h retrieves all $aRER_j^k$ abstracts from $LTSDB_h$ (from *External RER abstracts* table); based on that abstracts, RSS_h sends request for RER_j^k to each $EHRS_k$, which stores P_j clinical documents:
  Step 5.1. Using Inter-jurisdiction bus sends request to $ICEHR_k$;
  Step 5.2. $ICEHR_k$ sends request to EHR index service for all MS_i related to P_j;
  Step 5.3. $ICEHR_k$ sends request to RSS_k for RER_j;
  Step 5.4. RSS_k retrieves from $LTSDB_k$ RER_j (from *Guest RER* table) and send it to $ICEHR_k$;
  Step 5.5. $ICEHR_k$ sends MS_j^k and RER_j^k through Inter-jurisdiction bus to $ICEHR_h$, $ICEHR_h$ sends it further to RSS_h;
Step 1. RSS_h for each MS_j^k and RER_j^k using $aRER_j^k$ verifies its non-repudiation; after that RSS_h integrates all RER_j^k and RER_j^h into RER_j, which sends together with all MS_j^k to $ICEHR_h$;
Step 2. $ICEHR_h$ integrates all MS_j^k and MS_j^h into MS_j and sends it to query originator;
Step 3. Query originator, using RER XML file verification algorithm, verifies RER_j and MS_j. If correct, then query originator retrieves all clinical documents described by MS_j and calculates their hashes, which are finally compared with those in MS_j. If comparison is positive the non-repudiation of the EHR is proven.

4. Discussion and summary

The primary idea of the EHR is to gather all health information about a subject of care in one place. The security is one of the most important issues, when such systems are implemented in a large scale. Moreover, ensuring non-repudiation of the EHR will add a layer of security practically not available in a paper-based documentation (how to check in many healthcare sites if all paper documentation is available and not modified?). The verification algorithm of the EHR non-repudiation verifies all registry entries and then it is possible to verify all clinical documents, which are a content of the EHR. Only if everything is original and unaltered verification is positive. This would ensure patient that their medical documentation is intact.

The proposed algorithms operate on the logical level of EHR systems. They use addition algorithm, which operates in a registry logical level and is responsible for direct modification of RER. In the solution each patient has RER stored separately in each EHR system. Additionally, information about RER in external EHR systems is stored at the home system, so the home EHR system can supervise external systems and when a user sends request to the system for RER it gather all RERs from the external system and joins them into one. Also, when user asks for RERs in a patient's external system, that system forwards this to the home system and sends back to the user the answer from the home system. This is done to create one point of access for users. On the other hand, the repudiation could be ensured on the EHR system level i.e. each system would manage its own RER structure. This simplified solution would ensure the non-repudiation of the EHR inside one system instead of ensuring the non-repudiation of the EHR on the multi-system level.

The work was supported by finances of West Pomeranian Provincial Administration.

The work of T. Hyla is cofounded by European Union under European Social Fund and Polish State Budget, Operational Programme Human Capital Priority VIII, Action 8.2, Knowledge Transfer, Measure 8.2.2 "Regional Innovation Strategies", system project realized by Provincial Labor Office in Szczecin "Investment in the knowledge development mover of innovation in the region".

5. References

[1] Bates D. W.: Using information technology to reduce rates of medication errors in hospitals. BMJ, 2000, 320:788–791.
[2] Bates D.W., Teich J. M., Lee J., Seger D., Kuperman G.J., Ma'Luf N., et al: The impact of computerized physician order entry on medication error prevention. J. Am. Med. In-form. Assoc. 1999, 6, pp. 313–321.
[3] openEHR Foundation. The openEHR Reference Model – Support Information Model, 2007, [Online: http://www.openehr.org/svn/specification/TAGS/Release1.0.1/publishing/architecture/rm/ehr_im.pdf:], Release 1.0.1.
[4] CEN/ISO 13606-1:2009. Health informatics - Electronic Health Record Communication. Part 1: Reference Model, 2009.
[5] Hyla T., Pejaś J.: A security architecture of an inter-jurisdiction EHR system. Measurement Automation and Monitoring, 2009 nr 10, s. 823-826.
[6] IHE International, IT Infrastructure Technical Framework, Volume 1 (ITI TF-1) Integration Profiles. August 10, 2009. Revision 6.0 – Final Text.
[7] ANSI, ISO TS 18308 - Health Informatics - Requirments for an Electronic Health Record Architecture. s.l. : ISO, 2003.
[8] Van der Linden H., Kalra Dipak, Hasman Arie, Talmon J.: Inter-organizational future proof EHR systems: A review of the security and privacy related issues. International Journal of Medical Informatics, 2009, Vol. 78, pp. 141-160.
[9] ETSI, ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES), v1.4. June 2009.
[10] Pharow P., Blobel B.: Electronic signatures for long-lasting storage purposes in electronic archives. International Journal of Medical Informatics. 2005, Vol. 74, pp. 279-287.
[11] Blazic A. J., Klobucar T., Jerman B. D.: Long-term trusted preservation service using service interaction protocol and evidence records. Computer Standards & Interfaces. 2007, Vol. 29, pp. 398-412.
[12] Gondrom T., Brandner R., Pordesch U.: RFC 4998 Evidence Record Syntax (ERS). August 2007.
[13] Blazic A. J. et. al: Extensible Markup Language Evidence Record Syntax, Internet Draft. 2009.
[14] Merkle Ralph C.: Method of providing digital signatures. US Patent number: 4309569 Issue date: Jan 5, 1982.
[15] Hyla T., Pejaś J.: A method for long-term EHR metadata preservation in healthcare systems. Metody Informatyki Stosowanej. 3/2008, s. 125-134.

otrzymano / received: 14.07.2010
przyjęto do druku / accepted: 01.09.2010 *artykuł recenzowany*